1. Show that a subgroup $H$ of index 2 inside a finite group $G$ is normal.

Let $g \in G \setminus H$.

$gH = G \setminus H$.

Also, $Hg = G \setminus H$.

$gH = Hg$.

If $g \in H$, then $gH = H = Hg$.

So, $H$ is normal.

2. Exhibit a non-abelian group of order 21.

$\text{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$.

Let $f : \mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/7\mathbb{Z})$ be the homomorphism where $1 \mapsto 2$ followed by the isomorphism where $1 \mapsto \sigma_1$.

Let $G = \mathbb{Z}/3\mathbb{Z} \rtimes_f \mathbb{Z}/7\mathbb{Z}$.

Then $(1,0) + (1,1) = (2, \sigma_4(0) + 1) = (2,1)$, but $(1,1) + (1,0) = (2, \sigma_4(1) + 0) \neq (2,1)$ because $\sigma_4$ is not the identity.

So $G$ is a non-abelian group of order 21.

3. Show that a finite abelian group of linear operators on a finite-dimensional complex vector space has simultaneous eigenvectors forming a basis.

Let $A = \{A_i\}_{i=1}^n$ the group.

Then $\forall i, \ A_i^0 = I$.

So the minimal polynomial for $A_i$ divides $x^n - 1$.

$x^n - 1$ splits completely into distinct linear factors in the complex numbers.

This means so does the minimal polynomial for $A_i$.

Each $A_i$ is diagonalizable.
Base Case: \( \exists \) a basis of simultaneous eigenvectors for \( A_1, A_2 \).

\[
V = \sum_{\lambda \text{ an e-value for } A_1} V_\lambda \text{ where } V_\lambda \text{ is the } \lambda \text{ e-space for } A_1.
\]

Let \( v \in V_\lambda \).

\[
A_1 A_2 v = A_2 A_1 v = A_2 \lambda v = \lambda A_2 v
\]

So \( A_2(V_\lambda) \subseteq V_\lambda \).

Then \( A_2 \) is a linear operator on \( V_\lambda \).

Let \( f \) be the minimal polynomial on \( A_2 \) on \( V \).

Let \( f_\lambda \) be the minimal polynomial of \( A_2 \) on \( V_\lambda \).

Since \( f(A_2) \) vanishes everywhere, it vanishes on \( V_\lambda \).

By minimality, \( f_\lambda \) divides \( f \).

Since \( A_2 \) is diagonalizable, \( f_\lambda \) splits completely into distinct linear factors.

So \( f_\lambda \) splits completely into distinct linear factors.

\( A_2 \) is diagonalizable on \( V_\lambda \).

This is true for all \( \lambda \), so there is a basis of \( V \) where each element is in \( V_\lambda \) for some \( \lambda \) and is an eigenvector for \( A_2 \).

Then this is a basis of simultaneous eigenvectors for \( A_1, A_2 \).

Inductive Hypothesis: \( \exists \) a basis of simultaneous eigenvectors for \( A_1, \ldots, A_k \).

Inductive Step: \( V = \sum_{\lambda_1, \ldots, \lambda_k \text{ where } \lambda_i \text{ an e-value for } A_i} V_{\lambda_1, \ldots, \lambda_k} \text{ where } V_{\lambda_1, \ldots, \lambda_k} \text{ is the intersection of the } \lambda_i \text{ e-spaces for } A_i \).

Let \( v \in V_{\lambda_1, \ldots, \lambda_k}, i \in \{1, \ldots, k\} \).

\[
A_i A_{k+1} v = A_{k+1} A_i v = A_{k+1} \lambda_i v = \lambda_i A_{k+1} v
\]

So \( A_{k+1}(V_{\lambda_1, \ldots, \lambda_k}) \subseteq V_{\lambda_1, \ldots, \lambda_k} \).

Then \( A_{k+1} \) is a linear operator on \( V_{\lambda_1, \ldots, \lambda_k} \).
Let \( f \) be the minimal polynomial on \( A_{k+1} \) on \( V \).
Let \( f_{\lambda_1,\ldots,\lambda_k} \) be the minimal polynomial of \( A_{k+1} \) on \( V_{\lambda_1,\ldots,\lambda_k} \).
Since \( f(A_{k+1}) \) vanishes everywhere, it vanishes on \( V_{\lambda_1,\ldots,\lambda_k} \).
By minimality, \( f_{\lambda_1,\ldots,\lambda_k} \) divides \( f \).
Since \( A_{k+1} \) is diagonalizable, \( f \) splits completely into distinct linear factors.
So \( f_{\lambda_1,\ldots,\lambda_k} \) splits completely into distinct linear factors.
\( A_{k+1} \) is diagonalizable on \( V_{\lambda_1,\ldots,\lambda_k} \).
This is true for all \( \lambda_1,\ldots,\lambda_k \), so there is a basis of \( V \) where each element is in \( V_{\lambda_1,\ldots,\lambda_k} \) for some \( \lambda_1,\ldots,\lambda_k \) and is an eigenvector for \( A_{k+1} \).
Then this is a basis of simultaneous eigenvectors for \( A_1,\ldots,A_{k+1} \).
By induction, there is a basis of simultaneous eigenvectors for the whole group.

4. Show that \( x^4 + x^3 + x^2 + x + 1 \) is irreducible in \( \mathbb{F}_7[x] \).
\( x^4 + x^3 + x^2 + x + 1 = \Phi_5 \).

Roots of \( \Phi_5 \) are primitive 5th roots of unity.

If \( \Phi_5 \) has a quadratic factor, then it would have a root in \( \mathbb{F}_7^2 \).

But there are no elements of order 5 in \( \mathbb{F}_7 \).
So, \( \Phi_5 \) has no roots in \( \mathbb{F}_7 \).
\( \Phi_5 \) has no quadratic factors in \( \mathbb{F}_7[x] \).
\( \Phi_5 \) is irreducible.

5. Show that the ring of \( n \)-by-\( n \) matrices with entries in a field \( k \) has no proper two-sided ideals.

We need to show that if \( L \) is a non-zero ideal two-sided ideal of the ring, then \( I \in L \).
Define \( E_{ij} \) to be the matrix with 1 in the \( i \)th row, \( j \)th column, and 0s elsewhere.
Then \( E_{ij}E_{kl} = E_{il} \) if \( j = k \) and 0 otherwise.
Let \( M \) be a nonzero element of \( L \), \( m_{ij} \) the element in the \( i \)th row, \( j \)th column.
\( \exists \alpha, \beta \) where \( m_{\alpha\beta} \) is nonzero.
\[
\frac{1}{m_{\alpha\beta}} E_{aa} M E_{\beta\beta} = \frac{1}{m_{\alpha\beta}} E_{aa} \left( \sum_{i,j} m_{ij} E_{ij} \right) E_{\beta\beta} \\
= \frac{1}{m_{\alpha\beta}} \sum_{i,j} m_{ij} E_{aa} E_{ij} E_{\beta\beta} \\
= \frac{1}{m_{\alpha\beta}} \sum_{j} m_{\alpha j} E_{\alpha j} E_{\beta\beta} \\
= \frac{1}{m_{\alpha\beta}} m_{\alpha\beta} E_{\alpha\beta} \\
= E_{\alpha\beta} \in L
\]

\[E_{ja} E_{\alpha\beta} E_{\beta j} = E_{jj} \in L\]
So \(\sum_j E_{jj} = I \in L\).
So \(L\) is not a proper ideal.
There are no proper two-sided ideals.

6. Find all intermediate fields between \(\mathbb{Q}\) and \(\mathbb{Q}(\omega)\) where \(\omega\) is a primitive 12th root of unity.

Conjugates of \(\omega\) are \(\omega^5, \omega^7, \) and \(\omega^{11}\).

Let \(\alpha\) be the automorphism that sends \(\omega\) to \(\omega^5\).
\[\alpha^2(\omega) = \omega^{25} = \omega.\]

Let \(\beta\) be the automorphism that sends \(\omega\) to \(\omega^7\).
\[\beta^2(\omega) = \omega^{49} = \omega.\]

The Galois group is not \(\mathbb{Z}/4\mathbb{Z}\), so in is the Klein 4 group.

If \(\alpha(\omega^n) = \omega^n\), then \(5n \equiv n \mod 12\), so \(n = 0, 3, 6, 9\).
\[\alpha\text{ fixes } \mathbb{Q}(\omega^3) = \mathbb{Q}(i).\]

If \(\beta(\omega^n) = \omega^n\), then \(7n \equiv n \mod 12\), so \(n = 0, 2, 4, 6, 8, 10\).
\[\beta\text{ fixes } \mathbb{Q}(\omega^2) = \mathbb{Q}(e^{2\pi i/12}) = \mathbb{Q}(e^{\pi i/3}) = \mathbb{Q}(i\sqrt{3}).\]

\[\alpha \beta(\omega) = \omega^{11}.\]
So \(\alpha \beta\) fixes \(\mathbb{Q}(\omega + \omega^{11}) = \mathbb{Q}(\sqrt{3}).\)
The intermediate fields are \(\mathbb{Q}(i), \mathbb{Q}(i\sqrt{3}), \) and \(\mathbb{Q}(\sqrt{3}).\)
7. Exhibit two modules $M, N$ over $\mathbb{Z}[i]$ both with exactly 13 elements, and $M \not\cong N$ as $\mathbb{Z}[i]$ modules (Hint: $13 = 2^2 + 3^2$).

Let $M = \mathbb{Z}[i]/\langle 2 + 3i \rangle$. $N = \mathbb{Z}[i]/\langle 2 - 3i \rangle$. $|\mathbb{Z}[i]/\langle a + bi \rangle| = a^2 + b^2$, so $|M| = |N| = 13$.

Let $\varphi$ a module homomorphism.

$1 \not\in \langle 2 + 3i \rangle$.

$\varphi(2 - 3i) = (2 - 3i)\varphi(1) = 0$.

But $2 - 3i \not\in \langle 2 + 3i \rangle$, so then the kernel in nontrivial.

This means $\varphi$ is not an isomorphism.

So $M \not\cong N$. 